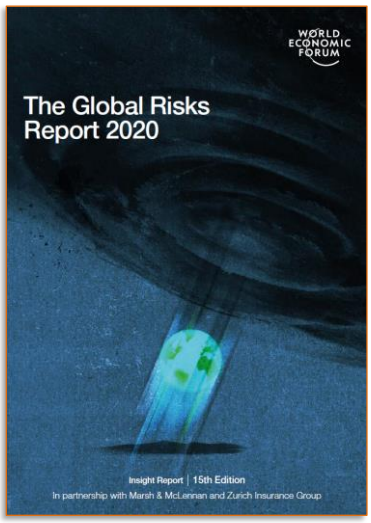
AGID | Agenzia per l'Italia Digitale

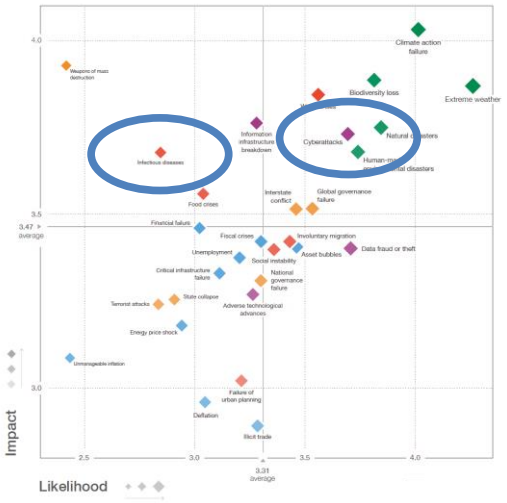
FormezPA

La sicurezza informatica nel contesto generale e nella PA

Corrado Giustozzi, AgID

Cybersecurity: solo una moda?





Sicurezza informatica negli anni '70

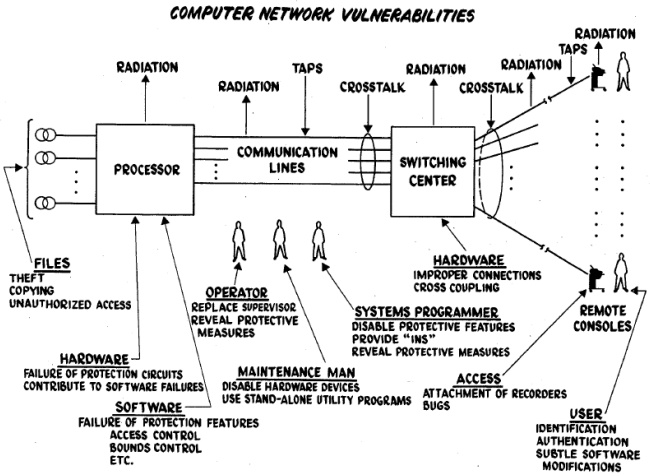
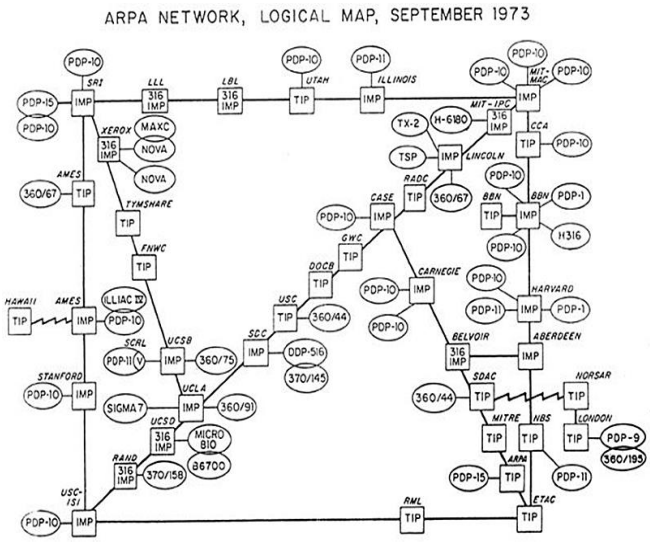


Figure 3

Fonte: "The Ware report", Rand Corp., 1970

3

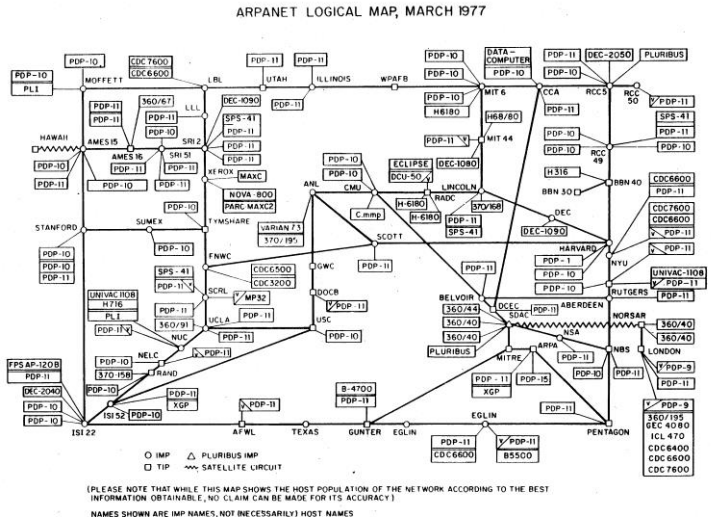
La prima ARPAnet



Fonte: Internet Society

4

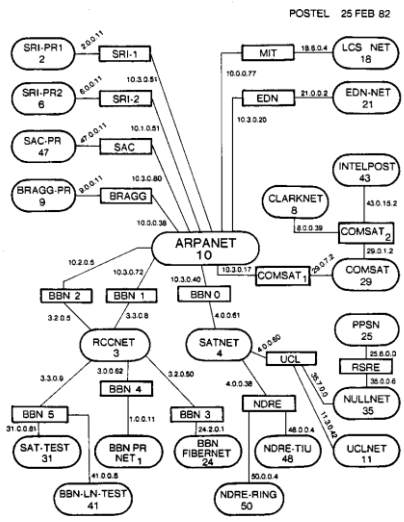
ARPANET negli anni ‘70



Fonte: Internet Society

5

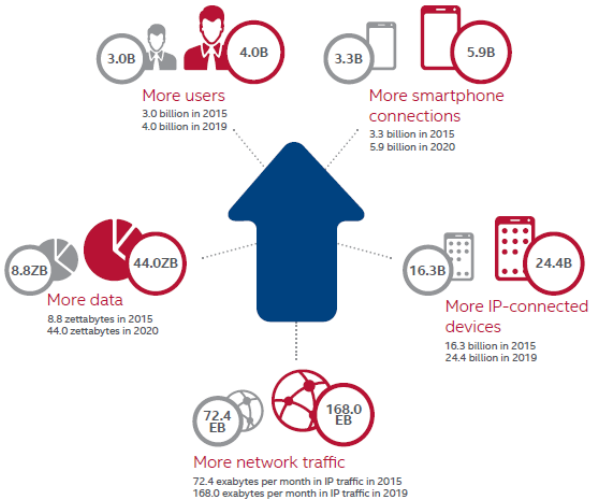
Internet nel 1982



Fonte: Internet Society

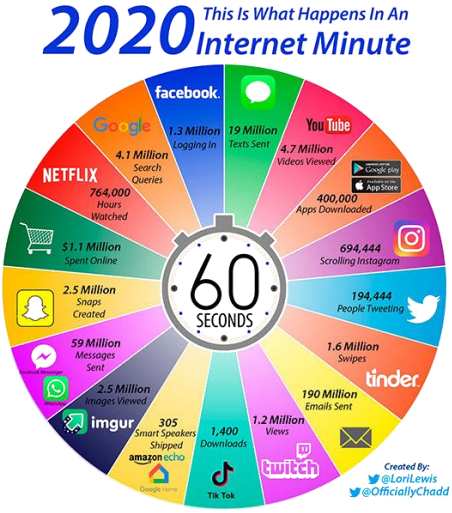
6

Aumento della superficie d'attacco



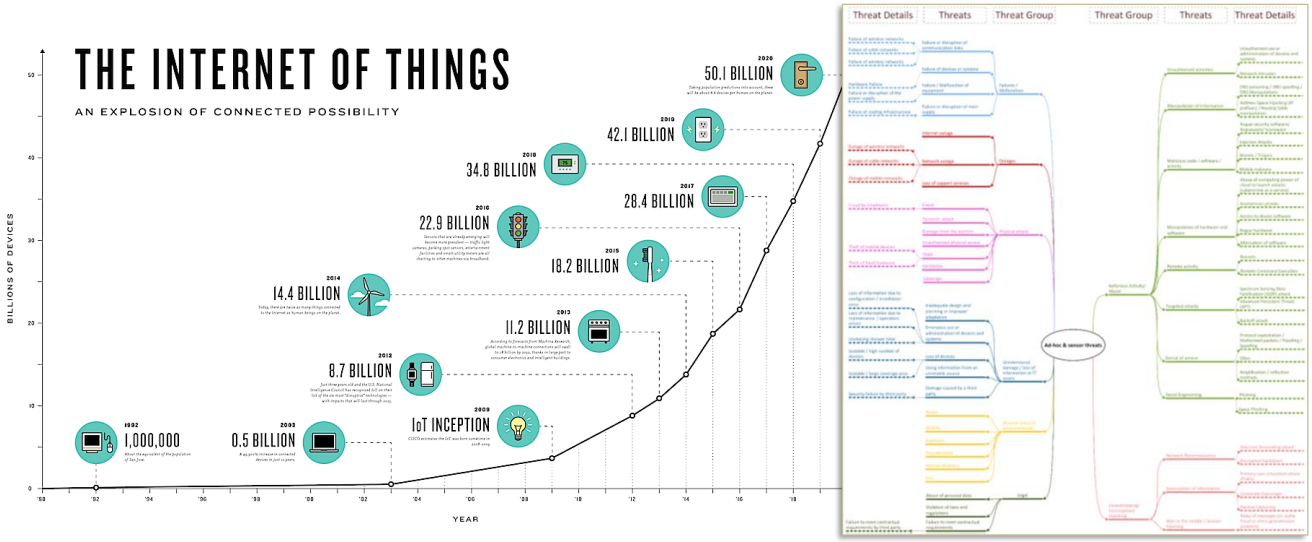
Fonte: McAfee Labs, 2015

I numeri di Internet, oggi e domani



- **Oggetti**: nel 2019 i dispositivi connessi in Rete hanno raggiunto un numero pari a tre volte e mezza la popolazione della Terra.
- **Traffico**: il traffico IP nel 2015 è stato di 72,4 HByte al mese. Nel 2019 è stato di 168,0 HByte al mese.
  (1 HByte = 10^{18} Byte, ossia un milione di TByte).
- **Utenti**: erano 3 miliardi nel 2015, sono diventati 4 miliardi nel 2019.

L'Internet delle cose e i nuovi rischi



9

Il bene supremo della società

- La nostra è la "società dell'informazione"
- L'informazione "tradizionale" è:
  - materiale e coincidente col suo supporto fisico
  - facilmente proteggibile con mezzi fisici
- L'informazione "moderna" è:
  - immateriale e svincolata dal suo supporto fisico
  - difficilmente proteggibile con metodi tradizionali
- L'informazione digitale può facilmente essere:
  - intercettata, copiata, trasportata, spostata, diffusa
  - modificata, contraffatta, falsificata, alterata
  - distrutta

10

Le proprietà fondamentali

- Riservatezza:
  - avere la certezza che una certa informazione possa essere conosciuta solo da chi ha il diritto a farlo
- Integrità:
  - avere la certezza che una certa informazione possa essere modificata solo da chi ha diritto a farlo e solo attraverso modalità note e verificabili
- Disponibilità:
  - avere la certezza che una certa informazione possa essere prontamente reperita ed utilizzata tutte le volte che si ha necessità di farlo

La sicurezza non è un *prodotto*

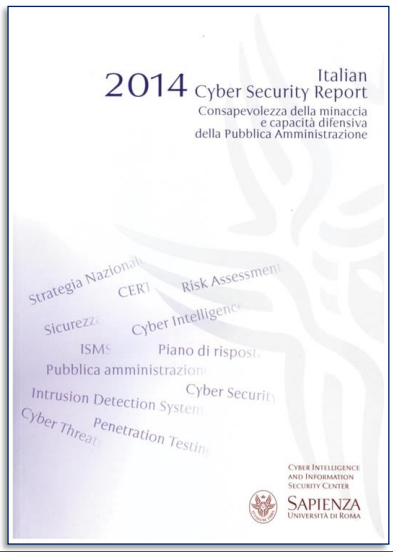
- La sicurezza è una **cultura aziendale**
  - va maturata con un'adeguata educazione
- La sicurezza è un **processo globale**
  - impatto trasversale sulle attività dell'organizzazione
- La sicurezza è un **servizio specializzato**
  - deve essere erogato da apposite strutture
- La sicurezza è una **risorsa da gestire**
  - complesso mix di competenze, risorse, prodotti

La sicurezza non è più *opzionale* (anche per la PA)

- Il GDPR:
  - impone una forte tutela dei dati personali
  - obbliga ad adottare rigorose ed adeguate misure di sicurezza
  - prevede anche sanzioni durissime!
- La Direttiva NIS e il Perimetro nazionale:
  - impongono la protezione dei propri servizi mediante adeguate misure di sicurezza
  - impogono obbligo di autovigilanza e denuncia degli incidenti significativi
  - prevedono dure sanzioni
- Il Codice dell'Amministrazione Digitale:
  - spinge verso il progressivo abbandono della carta a favore delle tecnologie digitali che richiedono adeguate misure di sicurezza

13

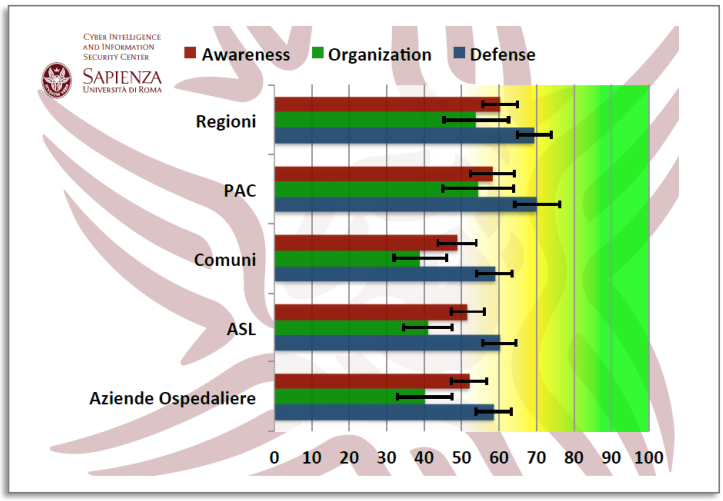
I razionali: la situazione nella PA

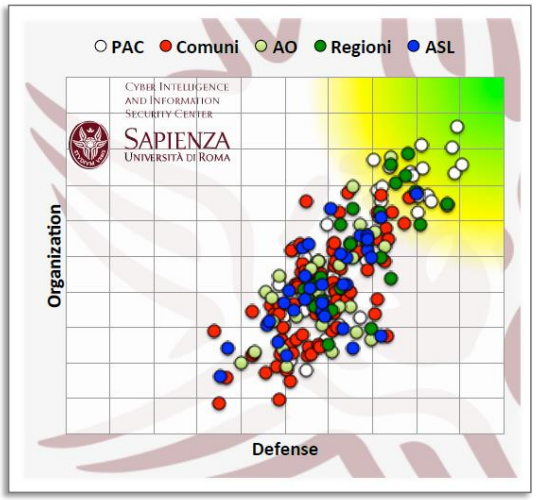


- Sicurezza basata sulle tecnologie
- Mancanza di strutture organizzative in grado di gestire gli eventi e rispondere agli attacchi
- Superficie d'attacco eccessiva
- Mancanza di una *baseline* comune di riferimento

14

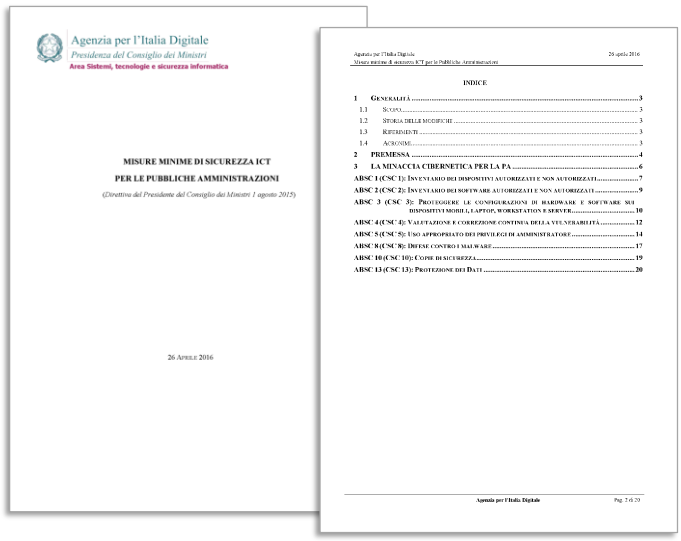
Una Pubblica Amministrazione vulnerabile





15

Le Misure Minime di sicurezza



- Già anticipate via Web sin da settembre 2016
- Emesse con circolare 18 aprile 2017, n. 2/2017
- Gazzetta Ufficiale (SG) n.103 del 5/5/2017
- Adozione obbligatoria entro il 31/12/2017
- Dovere d'ufficio del Dirigente responsabile IT (art. 17 CAD)

16

Obiettivi

- Indirizzare l'esigenza delle Amministrazioni fornendo loro, in particolare a quelle meno preparate, **un riferimento operativo direttamente utilizzabile** (*checklist*) nell'attesa della pubblicazione di documenti di indirizzo di più ampio respiro (linee guida, norme tecniche)
- Stabilire una **baseline comune** di misure tecniche ed organizzative irrinunciabili
- Fornire alle Amministrazioni uno strumento per **poter verificare lo stato corrente di attuazione delle misure di protezione** contro le minacce informatiche, e **poter tracciare un percorso di miglioramento**
- **Responsabilizzare le Amministrazioni** sulla necessità di migliorare e mantenere adeguato il proprio livello di protezione cibernetica ponendo il compito (e la relativa responsabilità) direttamente in capo al dirigente competente

Considerazioni ispiratrici

- Non reinventare la ruota ma basarsi su esperienze consolidate e condivise dagli esperti internazionali (SANS 20 / CSC)
- Indirizzare le caratteristiche e le esigenze specifiche delle nostre PP.AA.
- Minimizzare gli impatti implementativi (effort, costi)
- Requisiti in linea con le più diffuse e consolidate *best practice* di settore
- Armonizzare il quadro a valle del GDPR e della direttiva NIS

Tre livelli di applicazione

Minimo → È quello al quale **ogni pubblica amministrazione**, indipendentemente dalla sua natura e dimensione, **deve necessariamente essere o rendersi conforme.**

Standard → Può essere assunto come **base di riferimento nella maggior parte dei casi.**

Avanzato → Deve essere adottato dalle **organizzazioni maggiormente esposte a rischi** (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come **obiettivo di miglioramento** da parte di tutte le altre organizzazioni.

Le modalità di applicazione

- Il raggiungimento di elevati livelli di sicurezza, quando è molto elevata la complessità della struttura e l'eterogeneità dei servizi erogati, può essere eccessivamente oneroso se applicato in modo generalizzato.
- Pertanto ogni Amministrazione dovrà avere cura di **individuare al suo interno gli eventuali sottoinsiemi, tecnici e/o organizzativi, caratterizzati da omogeneità di requisiti ed obiettivi di sicurezza, all'interno dei quali potrà applicare in modo omogeneo le misure** adatte al raggiungimento degli obiettivi stessi.

Le famiglie di controlli

- **ABSC 1** (CSC 1): inventario dei dispositivi autorizzati e non autorizzati
- **ABSC 2** (CSC 2): inventario dei software autorizzati e non autorizzati
- **ABSC 3** (CSC 3): proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server
- **ABSC 4** (CSC 4): valutazione e correzione continua della vulnerabilità
- **ABSC 5** (CSC 5): uso appropriato dei privilegi di amministratore
- **ABSC 8** (CSC 8): difese contro i malware
- **ABSC 10** (CSC 10): copie di sicurezza
- **ABSC 13** (CSC 13): protezione dei dati

ABSC 1 (CSC 1): inventario dei dispositivi autorizzati e non autorizzati

- Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso
- Esempio:
  - Inventario delle risorse
  - Logging
  - Autenticazione di rete

ABSC 2 (CSC 2): inventario dei software autorizzati e non autorizzati

- Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione
- Esempio:
  - Inventario dei software autorizzati
  - Whitelist delle applicazioni autorizzate
  - Individuazione di software non autorizzato
  - Isolamento delle reti (air-gap)

AGID Agenzia per l'Italia Digitale 23 CERT-AGID

23

ABSC 3 (CSC 3): proteggere le configurazioni di hardware e software sui dispositivi

- Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.
- Esempio:
  - Configurazioni standard
  - Accesso amministrativo da connessioni protette
  - Verifica dell'integrità dei file critici
  - Gestione delle configurazioni

AGID Agenzia per l'Italia Digitale 24 CERT-AGID

24

ABSC 4 (CSC 4): valutazione e correzione continua della vulnerabilità

- Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.
- Esempio:
  - Verifica delle vulnerabilità
  - Aggiornamento dei sistemi

ABSC 5 (CSC 5): uso appropriato dei privilegi di amministratore

- Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.
- Esempio:
  - Limitazione dei privilegi delle utenze amministrative
  - Inventario delle utenze amministrative
  - Gestione delle credenziali delle utenze amministrative

ABSC 8 (CSC 8): difese contro i malware

- Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.
- Esempio:
  - Sistemi di protezione (antivirus, firewall, IPS)
  - Uso dei dispositivi esterni
  - Controllo dei contenuti Web, email

ABSC 10 (CSC 10): copie di sicurezza

- Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.
- Esempio:
  - Backup e verifica del restore
  - Protezione delle copie di backup

ABSC 13 (CSC 13): protezione dei dati

- Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti.
- Esempio:
  - Uso della crittografia
  - Limitazioni sull'uso di dispositivi removibili
  - Controlli sulle connessioni di rete/Internet

AGID Agenzia per l'Italia Digitale

FormezPA

GRAZIE PER L'ATTENZIONE

corrado.giustozzi@agid.gov.it

@cgiustozzi